Remarks and Arguments

The applicant has amended the claims to emphasize the inventive nature of the invention, without disclaimer of any subject matter changed or deleted.

Claim Objection

The objection to Claim 27 is gratefully noted and corrected by amendment to that claim.

Claim Rejections based on 35 USC § 102(b) and 35 USC § 103(a)

The rejections based 35 USC § 102(b), Teper (US Patent 5815665) will be discussed both with respect to 102(b), as well as with potential for 103(a) of obviousness of Teper in view of Micali (US Patent 5812670).

Amended Claim 1 consolidates original claims 1 and 2 which were rejected as being anticipated by Teper. Teper is an online brokering service that enables users of on-line service providers to interact with the on-line service providers while maintaining privacy with respect to their identity and personal information. Like the instant invention, Teper involves a closed authentication system, one where a prior relationship (enrollment) is required between a user and the authenticating party. However, Teper does not mediate interactions between authenticated users in the sense that the instant invention provides persistent mediation. In defining a Persistent Authentication and Mediation Service (PAMS), the application states "Mediation refers to the fact that communications between authenticated users pass through the PAMS giving the PAMS the capability to monitor the interaction and compile an audit trail" (page 7 line 11-13) and "Persistent refers to the fact that interaction remains mediated during the entire interaction under the PAMS, and messages persist until delivered." (ibid. lines 13-15).

Teper's brokering service does not mediate *either* the user or service provider in the sense defined above. The brokering service registers users and service providers and assigns them user name/passwords. In operation (during an interaction), the brokering service does not mediate interactions between users and service providers. In Teper, a user

contacts a service provider and is authenticated by means of a "pass through" protocol involving encrypted messages passed between the service provider and the user and between the service provider and the brokering service (see Fig.2 of Teper). The brokering service has no access to interactions between service provider and the user except as reported by the service provider (reporting billing events and changes in access rights – see Teper Figure 3), and this reporting occurs over separate connections maintained between each service provider and the brokering service. Thus Teper's brokering system does not mediate interactions between service providers and users, and its very structure (the broker having no direct access to the interaction and only receiving a report from the service provider over a second connection to which the user is not a party) precludes mediation as defined in the instant application. For clarity, amended claim 1 incorporates the definition of persistent mediation expressly into the claim.

Micali, discloses a method of transmitting anonymous traceable messages by handing the message off between trustees to keep the identity of a sender anonymous to a receiver, but traceable by cooperation of the trustees. Micali, doesn't discuss "open" or "closed" expressly, however, for applications over a distributed network (as opposed to special "self authenticating" cases such as use of a dedicated line or what Micali calls "backward travelling") Micali does not describe any system of pre-enrollment, verification, and storage of information about users as would be necessary for a "closed" authentication infra structure (supra). In fact, traceability could be achieved by a trustee knowing the address of the sender rather who sent the message (there could be many senders at an address). For transmissions over a distributed network, where Micali achieves actual authentication of the sending party (as opposed to just being able to trace his address) he relies on traditional Public Key *Infrastructure* where a party's identity is provided coupled to the parties public key encrypted by a trusted certification authority, by definition an "open" authentication infrastructure". Thus to the extent that Micali authenticates senders actual identity, if he does so, on a distributed network it only discloses an *inherently* open authentication infrastructure of conventional PKI. Also, Micali and Teper are such fundamentally different structures that the structure of Teper could not be modified to provide the mediation of Micali without completely redesigning

it and vice versa. Applicant also argues that it is not obvious to combine Micali and Teper for this reason (more detail under claim 3 where this issue was raised in the office action).

Claim 1, was amended for the purpose of consolidating original claims 1 and 2 since enrollment and verification by the authentication service are inherent in the closed infrastructure of the applicant's invention and to incorporate the definitions of persistent and mediation as used in the specification.

Amended claim 2 defines a further novel capability of the invention providing each user in an interaction with verified information about the other in an intelligible form before the interaction begins. This allows each user to decide whether to proceed with the other party before starting an interaction. Teper provides such information about the user to the service provider but not the reverse. For instance, a user doesn't really know that the party he reaches is not a spoof site since the user has no direct communication with the brokering service of Teper. Providing such information in an intelligible form in advance is antithetical to Micali because it destroys anonymity.

Claim 3 was rejected over Teper in view of Micali. Claim 3 was amended to add expressly that the audit trail is *directly* compiled by the on-line authentication service as part of the persistent mediation (see claim 1) and adds that the audit trail is available to the users during the interaction. While Micali does include an audit trail sufficient to trace a message, applicant respectfully argues that it would not have been obvious to one of ordinary skill in the art at the time of the invention, to modify Teper to include the audit trail of Micali in Teper, because Teper's brokering agent is constructed so that it has no direct access to user's interactions and only receives information about interactions as reported by service providers. In Teper the audit trail could only be compiled by one of the parties to an interaction, namely the service provider. Modification of Teper to include an audit trail compiled by the brokering agent would require a complete redesign of Teper's brokering agent. A suggestion to combine cannot require substantial

reconstruction or redesign of the prior art. (See, In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)).

Claim 4 was rejected as being anticipated by Teper. Teper mentions that "Although a one-way hash algorithm is preferred, it will be recognized that other types of cryptographic algorithms can be used to generate the response message, including public key and private key encryption algorithms." However, claim 4 refers to a pseudo-PKI system of the type which cryptographically camouflages a users private key in a software container. The camouflage technique is defined in the application as follows: "The software camouflage technique places the private key on the users site so that it is released when the user enters a correct password. "The private key is not merely encrypted with the password, however, *but it is said to be camouflaged because when incorrect passwords are inputted, in many cases a false but otherwise plausible private key is generated*(see page13 line 30 to page 14 line 6). A challenge message encrypted with a false key is identifiable when submitted for authentication". Applicant respectfully submits that nothing like this camouflaging was anticipated by Teper. Applicant has amended claim 4 to include the meaning of "camouflaged". This technique provides an added level of security comparable to a hardware smart card.

Claim 5 as amended emphasizes the pseudo PKI system as differing from Teper's reference as noted supra. Ordinary PKI involves a user having a matched private key and a public key. A first user encrypts a message with his private key and the public key of a second user. The public key is presented encrypted with a message certifying the identity of the first user in the form of a certificate from a trusted certification authority. The certificate may be decrypted with the published key of a trusted authority and verifies that the message was prepared by the first user. The second user may decrypt the message using his private key and the first users' public key. A PKI system is inherently an "open" system in that no prior relationship is needed between the first user and the authenticator (the second user). In a pseudo PKI system as defined in the application, the certificate containing a user's public key must be decrypted using a secret key under the exclusive control of the on-line authentication service. This mode of authentication of a

user to the authentication service is a "closed" system since the authentication service both certifies (enrolls) and authenticates the users. This is a substantial and unexpected advantage of the preferred embodiment of the invention since the instant authentication service need not store the users' passwords or other encryption key (in the instant invention, a user submits the certificate with his encrypted "public" key with his challenge response). In Teper's brokering service, the brokering service must store a user's key to validate that the hash was generated using a key valid for the user.

Claim 6 as amended emphasizes the ability for authenticated users to discover other authenticated users based on verified and non-verified credentials. This is more extensive than Teper's "SP directory" which is limited to user's searching for SPs.

Claim 7 as amended emphasizes a novelty of the invention, in that it is not limited to the traditional interaction between users and service providers, but enables peer to peer authenticated transactions between authenticated users communicating with a computing device running a browser.

Claim 8 as amended emphasizes a unique novelty of the preferred embodiment of the instant invention which places the audit trail available to the users *during* an interaction and allows them to select material for archival under control of the authentication service. This is a substantial difference from the audit trail of Micali that only allows tracing the identity of a sender after some event.

Claim 9 as amended emphasizes a unique feature the ability of authenticated users to submit dynamically variable credentials and to find other authenticated users based on these variable credentials as well as verified credentials. This is an important feature which was not previously known in the art.

Claim 10 as amended emphasizes a unique capability of the invention, the ability of groups of greater than two authenticated users to collaborate. Micali and Teper are expressly limited to two users.

Claim 11 and Claims 27-34 were rejected based on Teper in view of Micali, where Micali was relied on for the audit function. While Micali does include an audit trail so that a message can be traced, applicant respectfully argues as in claim 3 that it would not have been obvious to one of ordinary skill in the art to modify Teper to include the audit trail of Micali, because the structure of Teper prevents his brokering agent from having direct access to a user's interaction with a service provider. Teper's brokering agent is set up so that it has no direct access to user's interactions and only receives information about interactions as reported by service providers. Also, it is antithetical to the method of Micali to make the audit trail available in intelligible form during the interaction, since it would destroy anonymity.

Claim 11 as amended includes the definition of mediation in the claim and adds making the directly compiled audit trail available during the interaction. As mentioned in the preceding paragraph, the structure of Teper prevents modification to directly provide an audit function. Also, making the audit function available to the users during the interaction would destroy anonymity in Micali. Neither Micali or Teper suggest making an audit trail containing at least some of the mediated content of the interaction available to the users during an interaction. Yet, this is an important feature for authenticated business transactions.

Claim 27 has been amended to include the definitions of mediation, pseudo-PKI, and camouflaged private key as discussed in great detail supra in the discussion of claims 1, 3, 4, and 5. Neither Teper or Micali disclose a pseudo-PKI authentication system where the private key is camouflaged to protect the integrity of the private key and the public key is under the exclusive control of the authenticator. In PKI, a users public key is public and encrypted with identity information with the known public key of a trusted certification authority. In private key encryption both parties would use the same key to encrypt and decrypt messages. Using pseudo-PKI in the instant invention allows the added security of storing an encrypted public key at the user site and only forwarding it to the authentication service during authentication, thus no password or other private key

needs to be stored by the authentication service, a particular advantage for an on-line authentication service. As, mentioned supra in the introduction to claims 11 and 27-34, the structure of Teper cannot be modified to incorporate the direct audit of Micali's method. Also, it would be antithetical to Micali to provide the audit information during the interaction because it would defeat anonymity.

Claim 28-31 and 32-34 are patentable for the reasons stated for claim 27.

Claims 12 and 13 were rejected over Teper in view of Micali as above for claim 11 and further in view of VanTill (US 6404337). Van Till is a system and method for providing access to an unattended storage. Van Till describes use of a conventional Public Key Infrastructure involving a third party certification authority. Claim 12 has been amended to include the requirement for a camouflaged private key and encrypted "public" key which can only be decrypted with a key under exclusive control of the persistent authentication and mediation service, which differentiates it from Van Till (see discussions for claims 4,5, and 27, supra). Claim 13 utilizes the authentication system of claim 12.

Claims 14 – 21 were objected to as depending from a rejected base claim 13. Applicant believes he has now brought claims 11 into condition for allowance by amendment and argument, and thus cured the objection.

Claims 22-26, 35 and 36 were allowed.

Conclusion

Applicant now believes that claims 1- 21, and 27-31 and 33-34 as amended are now in condition for allowance, and respectfully requests reconsideration and allowance of all pending claims and Notice of Allowance for claims 1- 31 and 33-36 as listed above.

Please contact the undersigned attorney at (510) 785-8070 to discuss any aspect of this case.

Respectfully submitted

Howard E. Lebowitz

Howard E. Lebowitz
Registration No. 44,864
Attorney for the Applicant

June 6, 2004